مراجعة تقنية لتطبيق
SIMPLEX
للمحادثات الفورية



مؤسسة آفاق الإلكترونية
Electronic Horizons Foundation

مركز إنتاج الأنصار
ربيع الأول - 1447 هـ

المقدمة

بسم الله الرحمن الرحيم

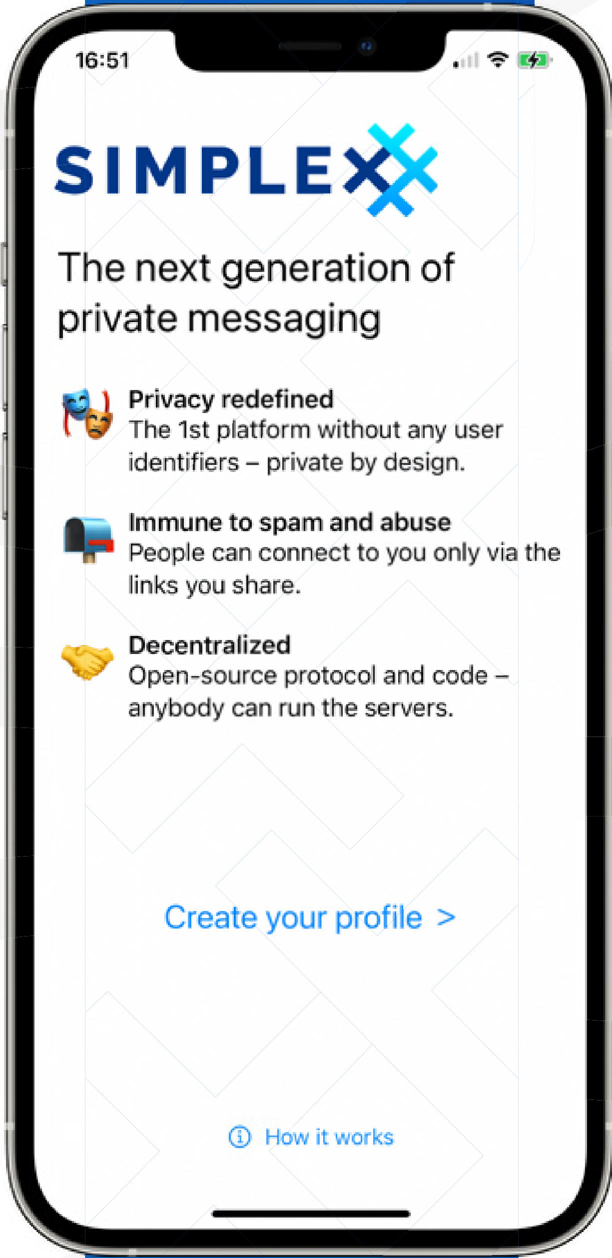
الحمد لله معز الإسلام بنصره، ومذل الشرك بقهره، ومصرف الأمور بأمره، ومستدرج الكافرين بمكره، الذي قدر الأيام دولًا بعدله، وجعل العاقبة للمتقين بفضله، والصلاة والسلام على من أعلى الله منار الإسلام بسيفه وعلى آله وصحبه ومن تبعهم بإحسان إلى يوم الدين.

نراجع في هذا المقال بشكل تفصيلي تطبيق المحادثات الفورية SIMPLEX ، سنتحدث عن:

اضغط على العنوان لتنتقل إلى الصفحة المطلوبة.



بدايةً ما هو تطبيق SimpleX؟



- هو تطبيق محادثات فورية لا يعتمد على معرف فريد للحساب كرقم هاتف أو بريد إلكتروني ولا حتى اسم معرف (user name).

- يعتمد التطبيق على شبكة لا مركزية بعكس كثير من التطبيقات المعروفة التي تعتمد على خوادم مركزية مثل تطبيق تيليجرام.

- يوفر التطبيق خدمة الرسائل المباشرة، أو المجموعات، كما يوفر الاتصالات المشفرة من الطرفين E2EE المحمية من خلال بروتوكول SimpleX Messaging الذي يستخدم خوارزمية التشفير Double Ratchet المقاومة للكم (Quantum Resistance).

- تم إطلاق التطبيق في عام 2021 من قبل شركة SimpleX Chat Ltd في المملكة المتحدة.

إيجابياته

-Part 1-

01 لا يوجد معرف حساب على التطبيق، ولا يحتاج رقمَ هاتف أو عنوانًا إلكترونيًّا (Email) للتسجيل، ولا يتم توليد رقم عشوائي حتى كمعرف للحساب.

02 استخدام التشفير التام بين الطرفين لكل ما يلي:

- الرسائل المباشرة بين حسابين.
- الصور والفيديوهات والملفات.
- المجموعات.
- الرسائل الصوتية.
- مكالمات الصوت والفيديو.

03 تبادل المفاتيح بطريقة out-of-band لمنع هجمات MITM.

04 درجة إضافية من التشفير على الخوادم غير المركزية للتطبيق، ويقتصر استخدام الخوادم للإبقاء على الرسائل المشفرة لحظيًّا إلى حين استلام الطرف الآخر للرسالة ثم تحذف من الخوادم.

05 ضمان عدم التلاعب بالرسائل من خلال أرقام تسلسلية للرسائل وإجراء تصديق للرسائل وتنبيه المستخدم في حال اختلاف الرقم التسلسلي، كما يتم عمل خلط للرسائل أثناء نقلها بين الطرفين حتى يصعب ربط الرسائل ببعضها.

إيجابياته

-Part 2-

06 إمكانية الاتصال اختياريًّا من خلال شبكة Tor.

07 حماية المعلومات الوصفية وجهات الاتصال للمستخدمين بحيث لا يتم مشاركتها مع خوادم التطبيق أو أي جهة، وتكون موجودة على جهاز المستخدم فقط.

08 خدمة الرسائل المؤقتة، والحذف التلقائي.

09 خدمة الرسائل الحية (Live messaging) التي توفر لك كتابة الرسائل بشكل مباشر دون حفظها.

10 استخدام الحسابات المجهولة (Anonymous Accounts) في المراسلات وبأسماء وهمية بشكل عشوائي، ويمكنك اختيار استخدام الاسم الفعلي للحساب أو اسم مجهول في كل محادثة أو مجموعة على التطبيق.

11 هناك إجراءات أمنية إلكترونية أخرى يتم تطبيقها في هذا التطبيق لكن لا يتسع المقال لذكرها.

سلبياته

01 المكالمات على نسخة الحاسوب من خلال WebRTC.

02 عدم وجود قنوات مثل تيليجرام.

03 وجود سقف لحجم الملفات المرسلة في المحادثات، ولكن هناك بروتوكول للتطبيق خاص بنقل الملفات اسمه XFTP يمكن استخدامه على أنظمة لينكس لإرسال الملفات كبيرة الحجم.

04 حـذف الملفـات بشـكل تلقائـي بعـد 48 سـاعة مـن رفعهـا، وتحتـاج لرفعهـا مـرة أخرى بعـد ذلـك.

المراجعات الأمنية التقنية للتطبيق

تمـت مراجعـة التطبيـق مـن الناحيـة الأمنيـة التقنيـة كالتشـفير واختبـار هجمـات MITM وغيرهـا مـن قبـل عـدة جهـات معروفـة في هـذا المجـال عالميًّا مثـل Trail of Bits، كمـا ينصـح مطـورو نظـام WhonixOS الشـهير باسـتخدام التطبيـق للمحادثـات الآمنـة



ختاماً

نـودُّ التنبيـه علـى قاعـدة تقنيـة أساسـية؛ وهي عدم وجـود تطبيق آمن 100% للتواصل عبـر الإنترنـت، كمـا أن احتمالية اكتشـاف ثغـرات فـي التطبيقـات والبروتوكـولات في أي لحظـة واردة، وقـد لا تكـون معروفـة، لذلـك يجـب الحـذر مـن إرسـال أي معلومـات شـخصية أو حساسـة عبـر أي تطبيـق تواصل عبـر الإنترنـت مهمـا اقتضـت الحاجـة.



